"Deficiencies in Security Assessment Methodologies"

MINIERI ASSOCIATES INTERNATIONAL

Worldwide Consultants & Engineers in Physical Security, Fire Protection & Life Safety

"PHYSICAL SECURITY ASSESSMENTS: Key Deficiencies in Common Methodologies"

By

Michael Minieri, CPP

Security Assessments of fixed facilities are the most common task performed by professional security consultants and other independent security practitioners throughout the world. From direct involvement in the formal assessments of more than 1000 sites over almost 40 years of working in nearly 30 countries, Michael Minieri - CPP and Principal Security Consultant with Minieri Associates (www.MinieriAssociates.com) – describes why many such undertakings often produce results that may be significantly misleading and extremely costly on several levels.

INTRODUCTION

The task is sometimes called a "*Security Vulnerability Assessment*", "*Security Risk Assessment*", "*Security Threat Assessment*" or any of several variations or combinations of the relevant terms. Regardless of its label, nearly all engagements of this nature are intended to include security "*risks*", "*threats*" and "*vulnerabilities*". Technically speaking, one could intentionally conduct an assessment of a specific element of security, to the exclusion of others if there were some good reason to do so. For purposes of this document, we will use the broader term of "*Physical Security Assessment (PSA)"* to be thorough, and also to distinguish Physical Security from its Information Technology (IT) cousin, commonly known as Logical Security.

Physical Security Assessments have probably been performed since practice of "protecting lives and property" first emerged as a profession. Written references to "defense settlements" date back to at least 1034. From the Latin words "*facere*" (to make) and "*fortis*" (strong), we derived words like *fort, fortifications* and *fortress.* That those who planned and designed these protective measures at the time must have "assessed" the threats, risks and vulnerabilities in the process – even if only informally – would seem inherent.

If PSAs in one form or another have been in existence since the advent of "security", so too has been the adage that "*No security is 100% effective".* If ever there existed a fortress that was actually attacked by a determined adversary and NOT eventually breached, no reference to it can easily be identified. There are countless examples in support of this adage, a most notable and historic case being that of Masada. Perched on a mountain top plateau in modern day Israel, this was once considered the ultimate in impenetrability, yet its various inhabitants throughout centuries were repeatedly defeated. SECURITY RISKS will always exist. Making those risks as low as reasonably practical is ultimately what security professionals do for a living. Under these circumstances an appropriate definition of a PSA might be as follows;

SECURITY ASSESSMENT: *"The task of identifying potential threats and the unacceptable risks of loss that could result from illegal or unwanted and intentional acts by any person (the "adversary") along with the countermeasures likely to effectively mitigate or otherwise reduce the probability or negative impact of such loss to an acceptable level"*

COMMON INDUSTRY PRACTICES

First, "common practices" are not necessarily the same as "best", "industry accepted" or "recognized" practices. That many may be doing it in a certain way – even getting paid to do it – makes it "common" but does not translate into "an effective way". Prior to the formalized methodologies of today, the quality of results from a PSA was entirely contingent upon the knowledge, skills, experience and abilities possessed by the individual Assessor. The only difference in the present day is that the aforementioned MUST also be accompanied by training and by the use of *some* methodology that has some basis in science, in order to be considered adequate under an expert peer review. Many PSAs are still conducted today without the aid of any formal methodology. Those days are past.

CONTEMPORARY FORMAL METHODOLOGIES

Like nearly every aspect of the security profession, PSAs underwent revolutionary changes as a result of the September 11, 2001 attack on New York's World Trade Center. In the United States in particular, Congress subsequently legislated mandatory PSAs for a significant number of industry segments that were considered to be "critical", including most forms of infrastructure. The requirements came in waves and included such sectors as

maritime, aviation, petrochemical, dams, water supplies and many more. Industry trade groups in most of the effected sectors worked to develop both security standards or guidelines and their own formal security assessment methodologies for their members. Some of these efforts were known to have been motivated by a desire to preempt government regulations in lieu of "voluntary" action by an industry. Some succeeded in this while others did not. Even in a large number of cases where federal legislation came along, the requirement to conduct PSAs was not accompanied by any mandate to actually take any corrective action. A common result was – and still is – that the PSAs identified *needs* for security upgrades or enhancements, but "compliance" was achieved simply by having performed the PSA itself. There were extremely few mandates requiring that effective security be implemented, thus missing the "objective" of it all. Perhaps such mandates were intended for a "second step" for political acceptability, but the "sense of urgency" has long ago faded.

There are now more than 100 formal "methodologies" for conducting a PSA, perhaps many hundreds. In 2003, the Office for Domestic Preparedness (ODP) within the Department of Homeland Security (DHS) published a reported from a study it commissioned regarding some of these methodologies by a group of industry experts. Entitled "*Vulnerability Assessment Methodologies Report*" the analysis provided a number of insights from a detailed evaluation of several dozen popular methodologies. For one, it established a 10-point criteria of essential elements in any methodology, and compared them against each version under consideration. They found that only 1 – Sandia Laboratory's Risk Assessment Methodology (RAM) met all ten of the desired criteria. While there is now Sandia RAM editions specifically directed toward numerous target markets, the fundamental principals involved are common across the board. Perhaps of the greatest significance, was their conclusion regarding the use of "numerical formulas" in attempting to calculate risk (emphasis added);

"*Clearly, the numerical values assigned were in nearly every case ordinal, at best. Thus,* ***those methodologies that did calculate a risk value did so using mathematical techniques that were not supported by the scaling assumptions involved****. In all mathematical calculations, the scales presented an order, not relative values. Hence, a reduction in risk by one unit – for example from 23 to 22 – may or may not be comparable to a similar reduction in risk by one unit from 5 to 4."*

Having either utilized – when mandated by a client – or personally reviewed a large number of standard methodologies, including several software based programs, the report's conclusion referenced above is confirmed through experience.

In all probability some degree of "subjectivity" underlies the "math" in at least many of the methodologies that have a significant "numerically calculated" component. It is very tempting for a developer to pursue mathematical formulas as either a key element or even the fundamental principal when producing a formal program, either software or paper based. IF it could be done so as to produce CONSISTENTLY ACCURATE AND USEFUL results, it would start a paradigm shift for the task of conducting a PSA. In that an Assessor's report is the primary tool for "communicating" the results of a PSA to the stakeholders, alpha and numeric representations of data can still be one efficient technique. It is particularly useful in highlighting information for use in prioritization of subsequent action, for example.

The frequent deficiency in such methodologies is that stakeholders tend to mistakenly assume that using mathematical science translates into *credibility* when it clearly does not. Where there is "subjectivity" behind any alpha or numeric representations, the underlying basis should ALWAYS be described along with it.

THREE ABSOLUTE ESSENTIALS

1. VULNERABILITY
2. NEGATIVE IMPACT
3. PROBABILITY

Though not in any particular order of importance, no PSA can be complete and valid without all 3 of the above elements, among others. Of these essential elements, it can be argued that only financially related "negative impact" can be ascertained *objectively* for reasonable and practical purposes. The valuation of an asset that may be damaged or destroyed is a common task in most any business, more often for non-security related reasons.

Probability might be addressed objectively, as an expression of mathematically calculated "odds of occurrence" for example. This is a task at the heart of the job of the actuarial professional, with insurance companies being the primary user. To be valid and useful, such calculations require a significant and substantial amount of related and factual historical data. With respect to the probability of most security related events, such data would be extremely difficult – if not impossible – to assemble. Therefore, within the scope of a PSA, probability remains in the realm of "subjective" to one degree or another.

There can be little argument that *vulnerability* is anything other than *subjective*. Put two or more security professionals together in a room and one can easily elicit more conflicting opinions than there are people.

Many popular formal methodologies – perhaps surprisingly – will include only 2 of the 3 elements, with "*probability*" being the most frequent omission. Consider that being vulnerable to an event that would cause a severe loss ("negative impact"), may not automatically justify a huge capital expenditure on additional security, if the likelihood ("probability") of that event is so remote that the risk is still acceptable. Nearly all facilities are vulnerable to total destruction by alien spacecraft, but no one has invested in effective countermeasures against that event so far! This example highlights the fact that many security professionals mistakenly take the approach that every vulnerability must have a security countermeasure applied, resulting in an extreme disservice to the PSA stakeholders. In a known case, more than 600 facilities were assessed using a software program that did not appropriately factor *probability*.

Security Risk Management is a sub-set of the more encompassing practice of Risk Management. Risks can be *transferred* to others (such as through insurance), can be *mitigated* (often in several alternative ways) or can be *accepted* (such as when the other choices are impractical) and this applies to Security Risks as well. It is among the goals of a good PSA to consider all of these and to recommend the solution that best meets the needs of the stakeholders. **THE MOST COMMON error** by an Assessor is to BEGIN the process with a focus on *VULNERABILITY*. This should be one of the last steps and this tendency could be a result of the security background of most who conduct PSAs. Most security practitioners have – at least at some point – been professionally focused on security products or services that might be used for mitigation. Not all seem capable of "*thinking beyond THAT box*".

Mitigation of vulnerabilities does not always require "more security" and sometimes the best solution is not technically a "security" issue at all. For example, establishing REDUNDANCY to an asset – if practical -might greatly reduce the target attractiveness to an adversary or might reduce or eliminate the degree of criticality.

CONCLUSION

This might rightly be summarized in fairly simple terms; while some formal security assessment methodologies can contribute very positively to the desired result, no training or methodology yet exists that can compensate for any lack of knowledge, skills, abilities and experience on the part of the Assessor whose boots are on the ground.

ABOUT THE AUTHOR

Michael Minieri is an independent, professional security consultant and founder of Minieri Associates, and is certified in Sandia RAM. He recently completed his 4th career project involving security assessments of more than 100 facilities for a single government entity of private sector enterprise, and has conducted assessments of more than 1000 sites through smaller engagements. Mr. Minieri is the developer of the *Minieri Associates Security Assessment Methodology* (MASAM®), an exclusive custom protocol derived and refined from his collection of the best elements of all the methodologies he has used or evaluated. To contact or learn more about him or the firm, or obtain permission to reprint this document visit www.MinieriAssociates.com

